Per 1 augustus 2022 treedt versie 3.0 van de beveiligingsnorm ICT-beveiligingsassessments DigiD in werking. In deze versie is norm B.01 toegevoegd. Vooruitlopend op de update van de NOREA DigiD Handreiking die in september zal worden uitgebracht, is in voorliggend document de nadere toelichting en de testaanpak door de IT auditor t.a.v. norm B.01 beschreven.

Ref	Beveiligingsrichtlijn	Type	Handreiking voor de IT auditor
B.01	De organisatie formuleert een informatie-beveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatie-gerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer. Doelstelling: Het zorgen voor specifieke management aandacht in het beveiligingsproces voor de webapplicaties van de organisatie.	Governance	Betrokken rol(len): • Applicatie-, hosting- of SAAS leverancier. • Houder van DigiD aansluiting. Scope: • De DigiD webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Nadere toelichting: De focus ligt op het vaststellen dat het eigenaarschap van de DigiD webapplicatie is georganiseerd, bevoegdheden aan de eigenaar zijn toegekend en dat de organisatie beschikt over een geactualiseerd (minimaal eenmaal in de 5 jaar dan wel bij grote organisatiewijzigingen en/of wijzigingen in de ICT) informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid bevat (expliciet) het beleid over de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van de DigiD webapplicatie en/of de infrastructuur voor het netwerksegment met de DigiD webapplicatie. Diepgang: • Opzet en bestaan van de beheersingsmaatregelen. Test aanpak: • Stel vast dat de houder van de DigiD aansluiting het eigenaarschap t.a.v.de DigiD webapplicatie adequaat op een hoog organisatorisch niveau heeft ingericht en dat de eigenaar passende bevoegdheden heeft. • Stel vast dat in het informatiebeveiligingsbeleid, of in een hiervoor apart ontwikkeld beleid, expliciet aandacht is besteed aan het stelsel van beveiligingsmaatregelen t.a.v. webapplicaties en/of de infrastructuren voor de netwerksegmenten met webapplicaties in het algemeen, en DigiD en andere authenticatie- en identificatiediensten in het bijzonder. • Stel vast dat dataclassificatie (zie U/WA.05), toegangsvoorziening (zie U/TV.01) en kwetsbaarhedenbeheer (zie U/PW.07, U/NW.06, C.03 en C.09) zijn geadresseerd. • Stel vast dat het informatiebeveiligingsbeleid door het verantwoordelijk hoger management is vastgesteld en actief wordt uitgedragen, alsmede bekend is bij functionarissen betrokken bij webapplicatie gerelateerde onderwerpen. • Stel vast dat het verantwoordelijk hoger management periodiek rapportages ontvangt inzake informatiebeveiliging en indien nodig hierop acteert. • Stel vast dat het informatiebeveiligingsbeleid wordt geüpdatet conform de beleidscyclus van de organisatie, doch minimaal eens in de 5 jaar. Bij (tussentijdse) grote wijzigingen dient het informatiebeveiligingsbeleid te worden geactualiseerd. • Interview de verantwoordelijke functionarissen.